Using the System Connector to Build a Strong Security Posture

Gus Green, Automation Manager

 ©2018 OSIsoft, LLC

Conference Theme & Keywords



©2018 OSIsoft, LLC

Agenda

About Biogen

Understanding Cyber Attacks

Example Industrial Network Scenarios

Actions and Focus

Replication and the PI System Connector

©2018 OSIsoft, LLC

About Biogen

One of the pioneers in biotechnology, Biogen today has the leading portfolio of medicines to treat multiple sclerosis, has the first and only approved treatment for spinal muscular atrophy and is at the forefront of research in neuroscience. Biogen also manufactures and commercializes biosimilars of advanced biologics.

Led by world-class research and development, Biogen uses novel science and leading-edge technologies to create, commercialize, and manufacture transformative therapies.



©2018 OSIsoft, LLC

Challenge



•Today's control systems are increasingly networked, internal customers need access to more and more data



Networking makes data more available but at the same time those systems become more vulnerable to security threats



Intellectual property and confidential data often reside on PI - how do we reduce vulnerability?

©2018 OSIsoft, LLC

Do We Take Cyber Security for Granted?

It will never happen to me...

Antivirus will protect me…

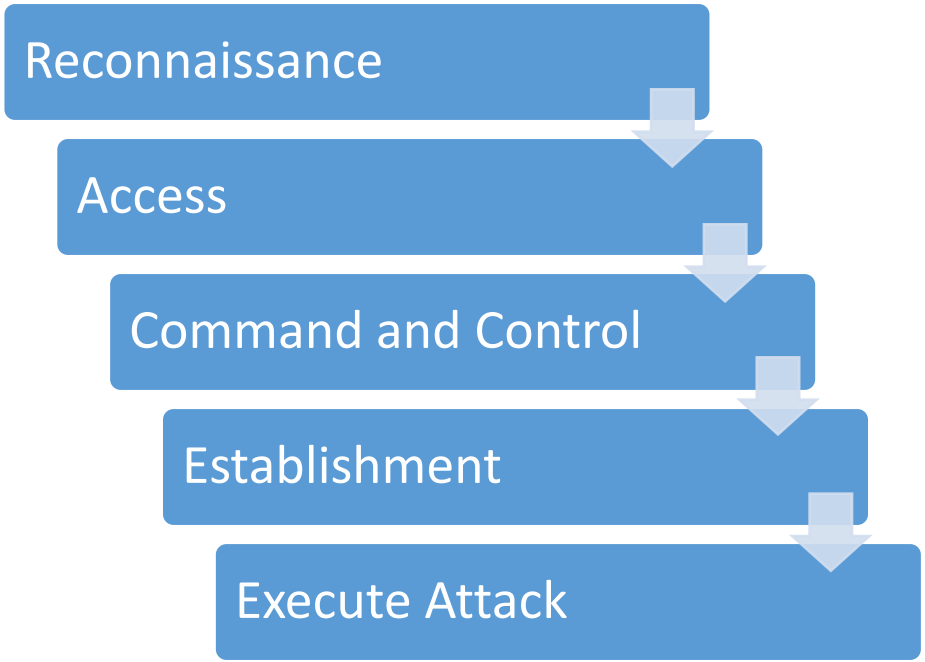
Nation states would not target my company…

My network is behind a firewall…

I am protected…

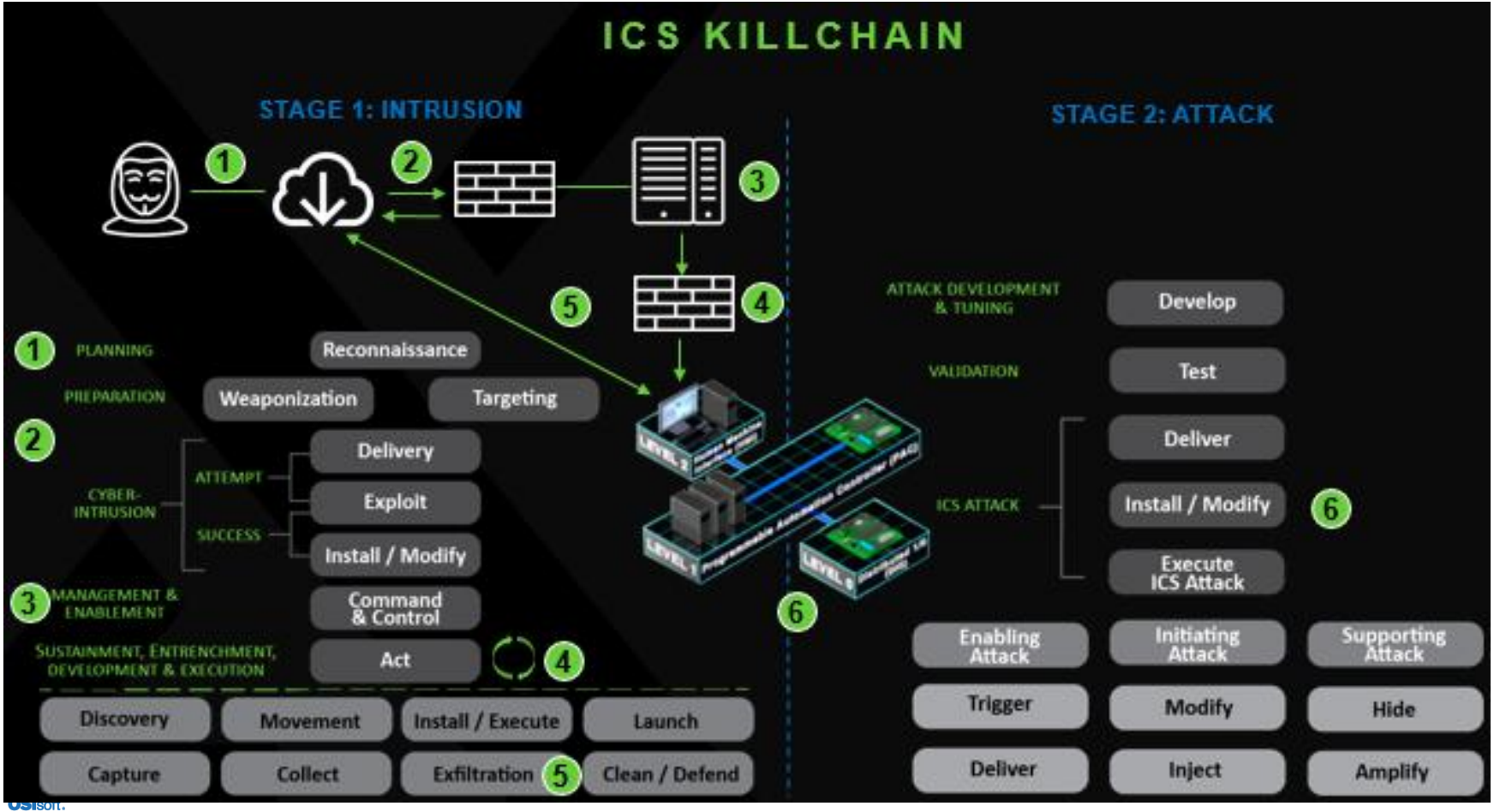
©2018 OSIsoft, LLC

Attack Stages



The most effective stage to prevent attack is to prevent access. Once the network has been breached your remediation devices will have to keep up with movement through the network in which many times that won't be fast enough.

©2018 OSIsoft, LLC



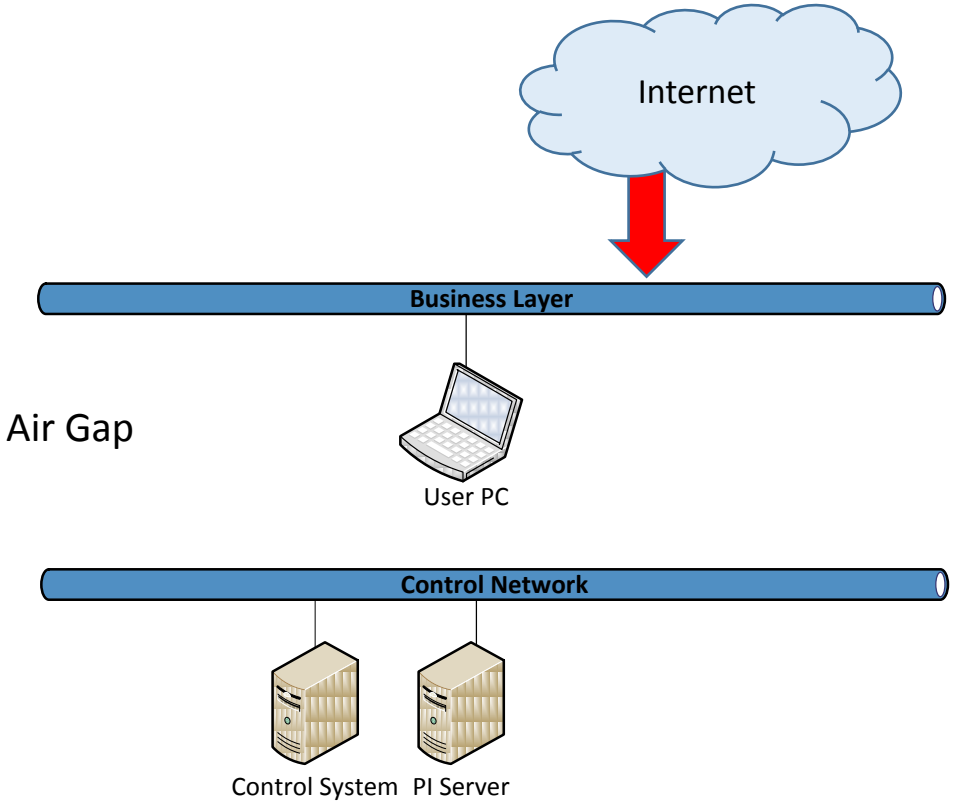
©2018 OSIsoft, LLC

Simple Control Network

Main Points

Pro:
Control network not vulnerable from outside attack.

Con:
Security requirements such as an air gap protecting the manufacturing systems creates a barrier to accessing and leveraging data widely beyond the shop floor.



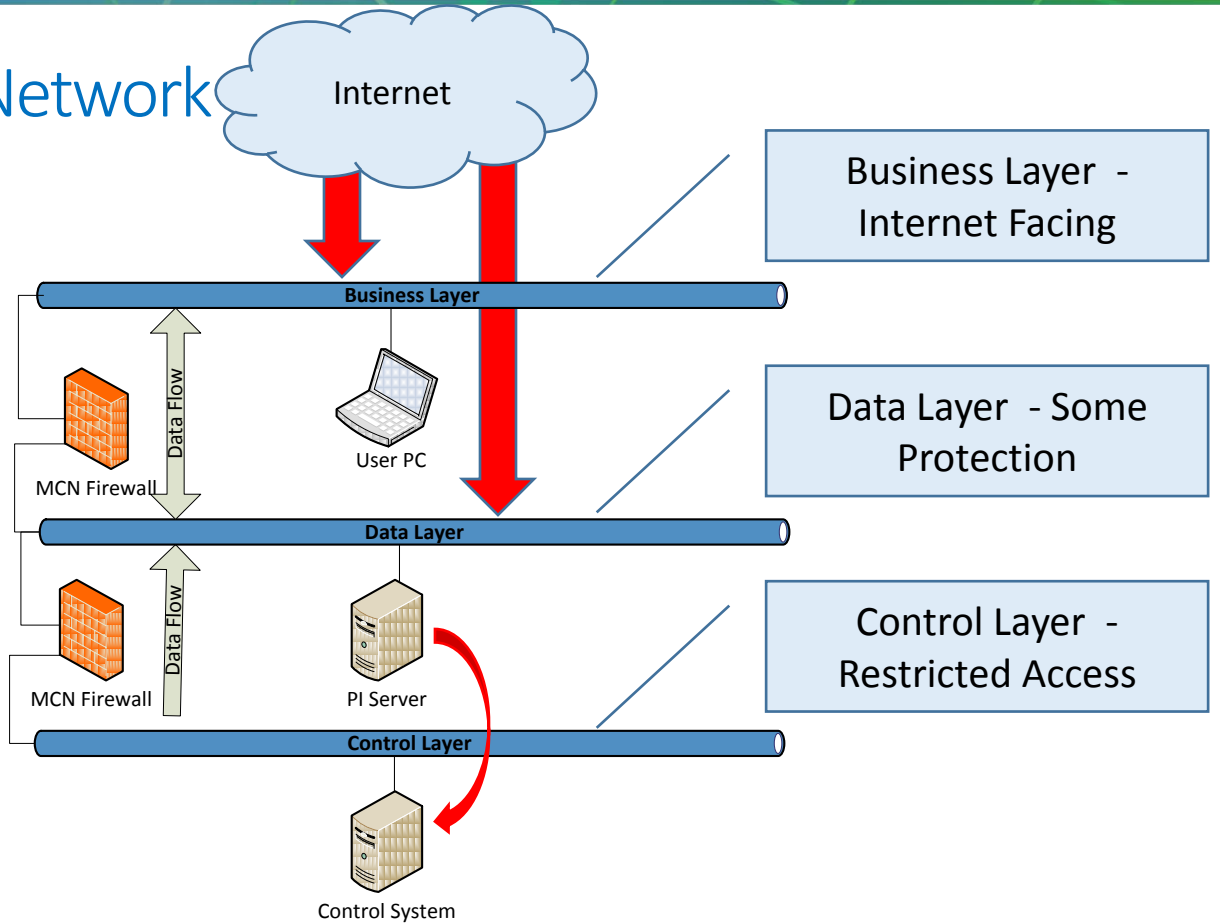
©2018 OSIsoft, LLC

Accessible Control Network

Main Points

Pro:
Data is accessible to users on the Business Layer
Control Layer is isolated from the internet.

Con:
Bidirectional communication allows wide access from threat actors.
2-way communication used between individual servers on Data Layer to Control Layer.



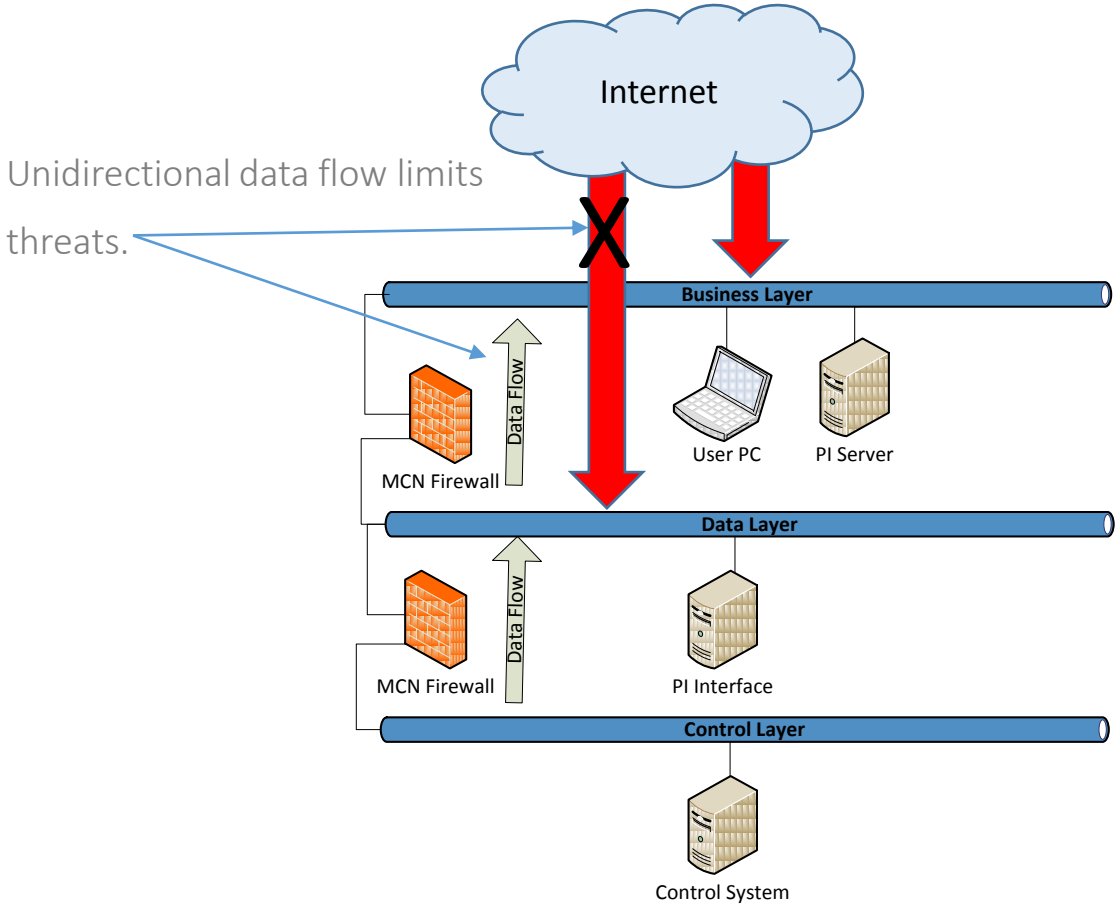
©2018 OSIsoft, LLC

Enterprise PI Scenario

Main Points

Pro:
Data flow is always moving up through the network.
Data is accessible to users.

Con:
PI Server acts as only a traditional historian.

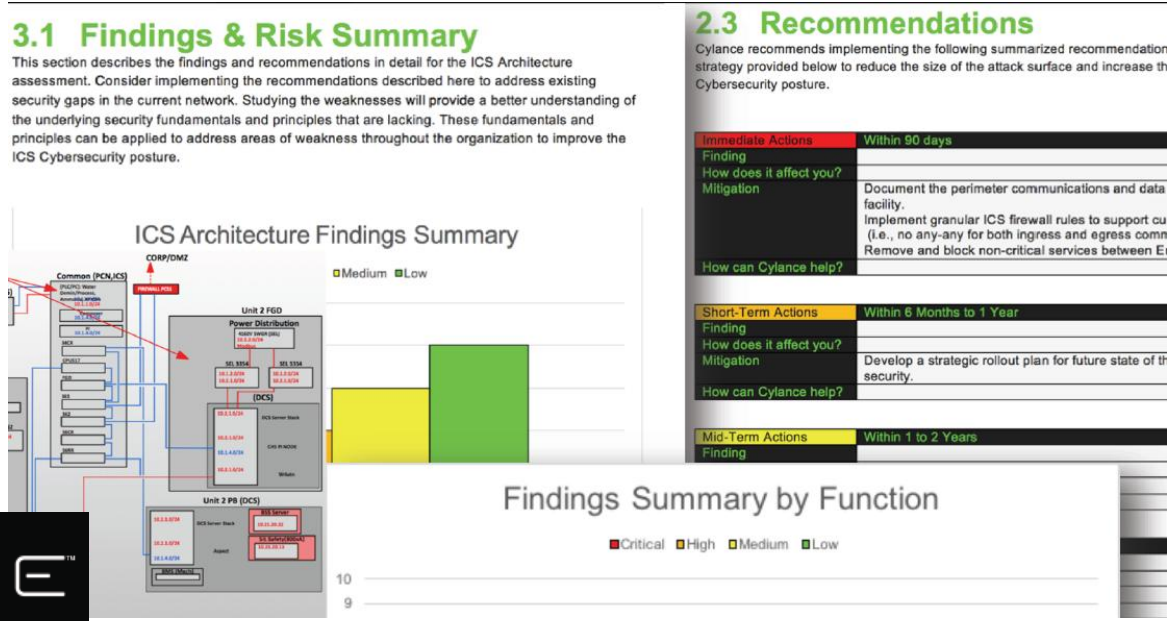


©2018 OSIsoft, LLC

Cyber Security Assessment

Assessed different categories such as:

Network Architecture, Security Policies, Configuration Management, Physical Security, Patch Management, etc.



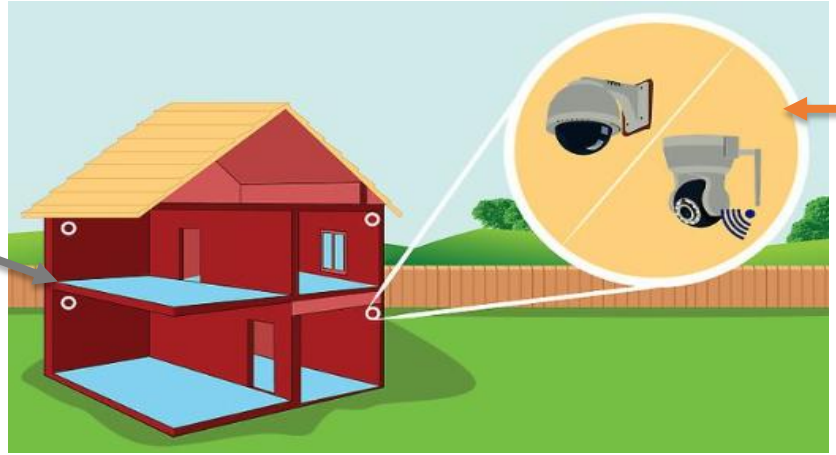
CYLANCE CONSULTING

©2018 OSIsoft, LLC

Preventing Access

The best prevention of a network attack is to not let the threat actor in!

Open firewall ports are like opening up the walls to your house



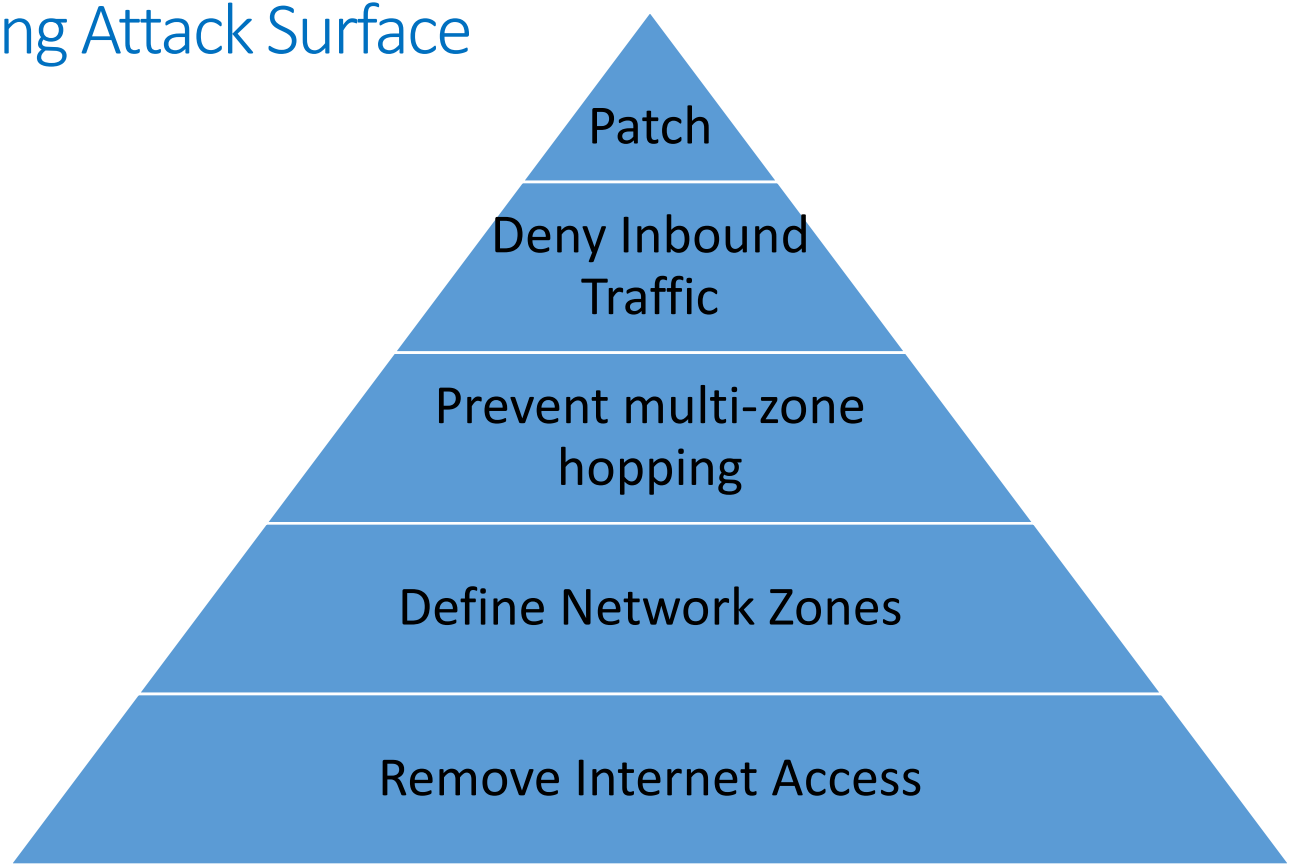
Intrusion protection systems monitoring open doors are not 100% effective

Antivirus is effective but only at remediation!

Antivirus, IDS devices and other traditional IT security measures aren't effective enough when dealing with safety systems and production!

©2018 OSIsoft, LLC

Reducing Attack Surface



©2018 OSIsoft, LLC

Network Zones Defined

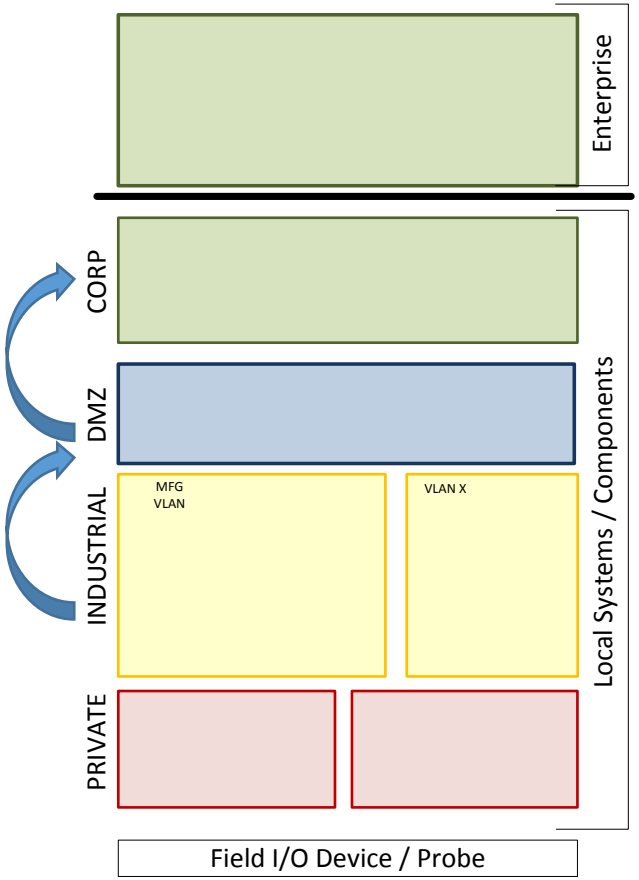
Enterprise/Business Layer – Will consist of site-based and Enterprise business layer

De-Militarized Zone (DMZ) – Used for access to the MCN

Industrial Layer – Restricted MCN

Private Layer – Private networks for control systems

Approach is basically a simplified Purdue Model.



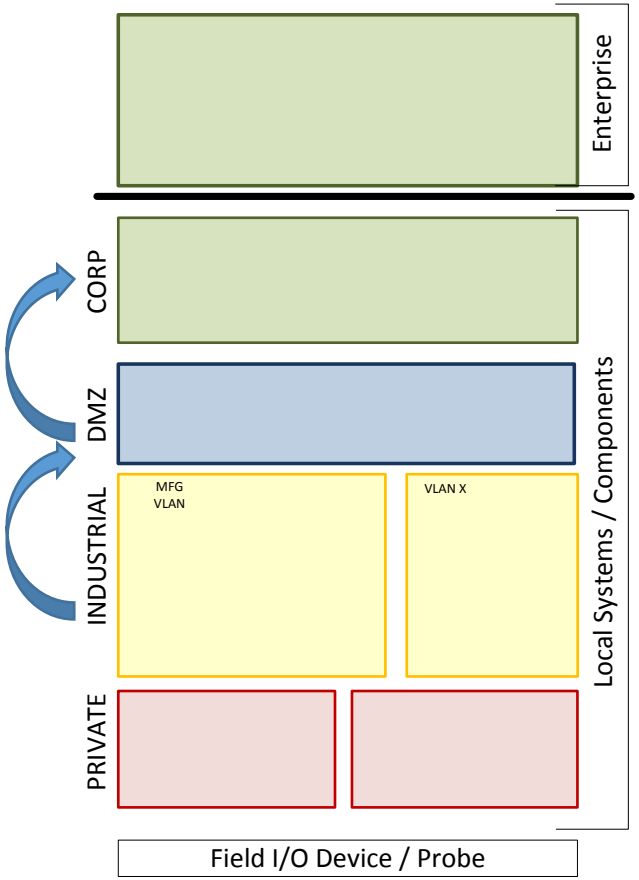
©2018 OSIsoft, LLC

Drawing a Line in the Sand

Fundamental Philosophy

- All communication stops within the DMZ
- Communication flow is outbound
- Access to DMZ is only inbound via 2-factor authentication or Application Virtualization

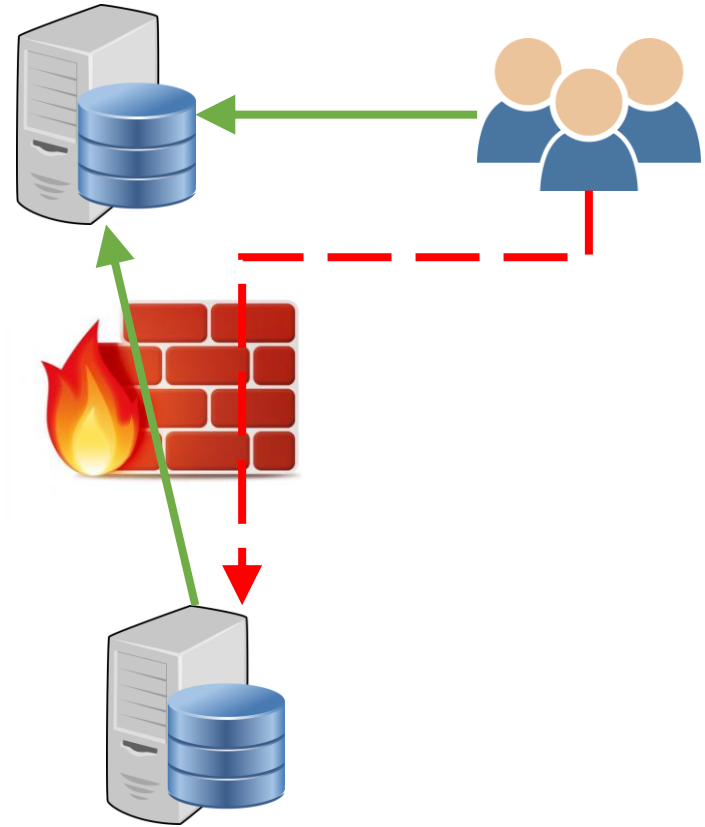
Reduce Inbound Attacks!



©2018 OSIsoft, LLC

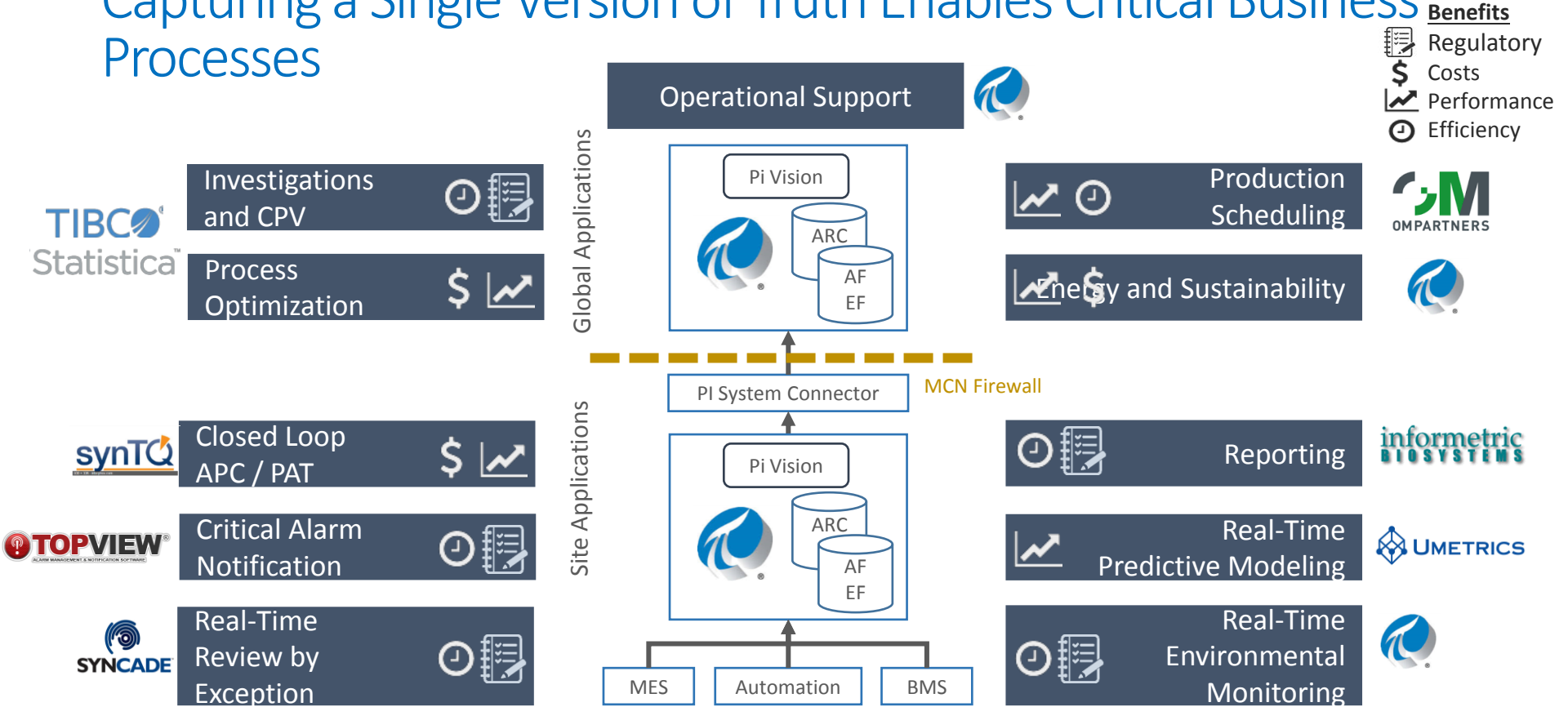
Replication

- Replication is what brings data to users via outbound connection to enterprise level server
- Removes need to punch an inbound hole in the firewall for data access
- Business systems access replicate in the enterprise



©2018 OSIsoft, LLC

Capturing a Single Version of Truth Enables Critical Business Processes

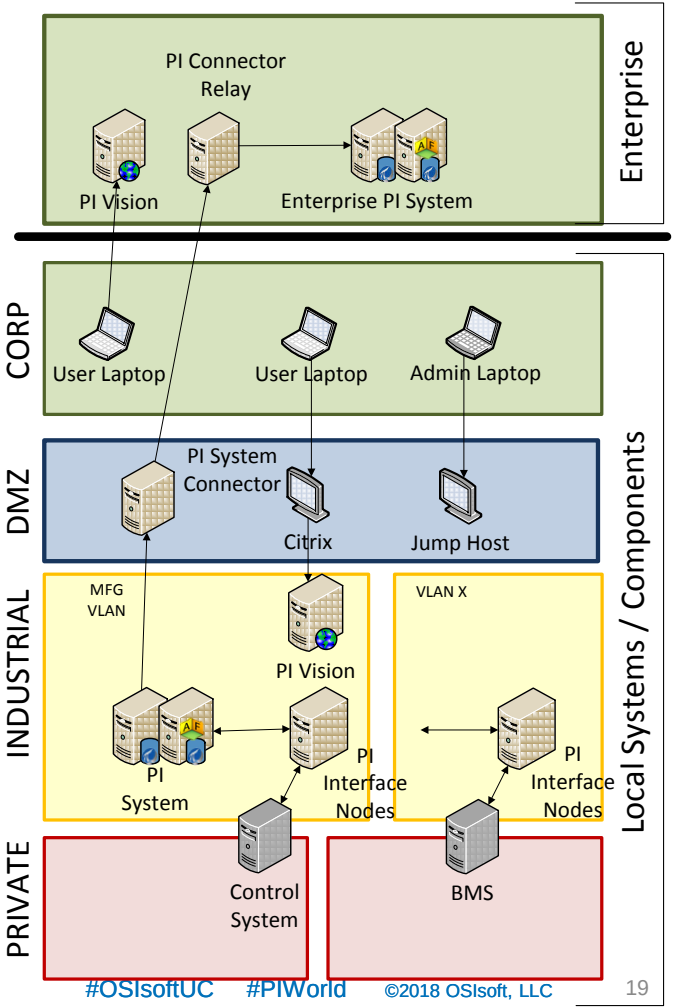


©2018 OSIsoft, LLC

Secure PI System Architecture

Architecture allows for:

- Data access where needed at the business layer
- Protection to the site master PI Server
- Resiliency during a WAN outage
- Replicates important data from other restricted systems through PI

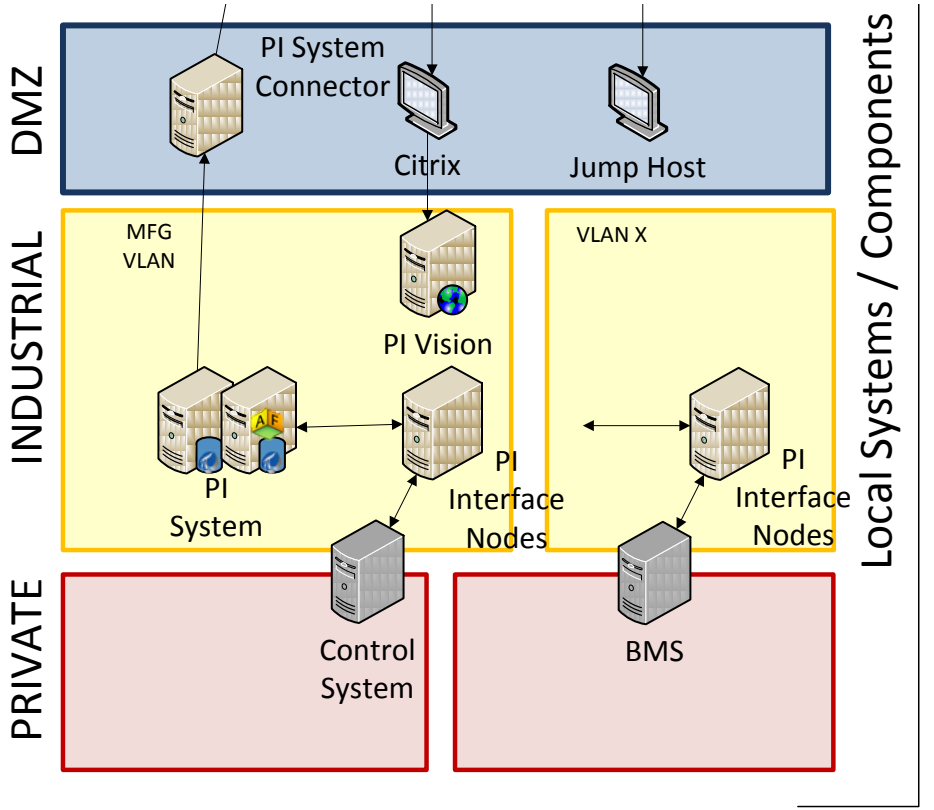


©2018 OSIsoft, LLC

PI System Connector Architecture Within MCN

The PI System Connector is installed in two pieces comprising of the PI System Connector and the PI Connector Relay. The PI Data Collection Manager, a web based app, is used to monitor and configure both the PI System Connector and PI Connector Relay.

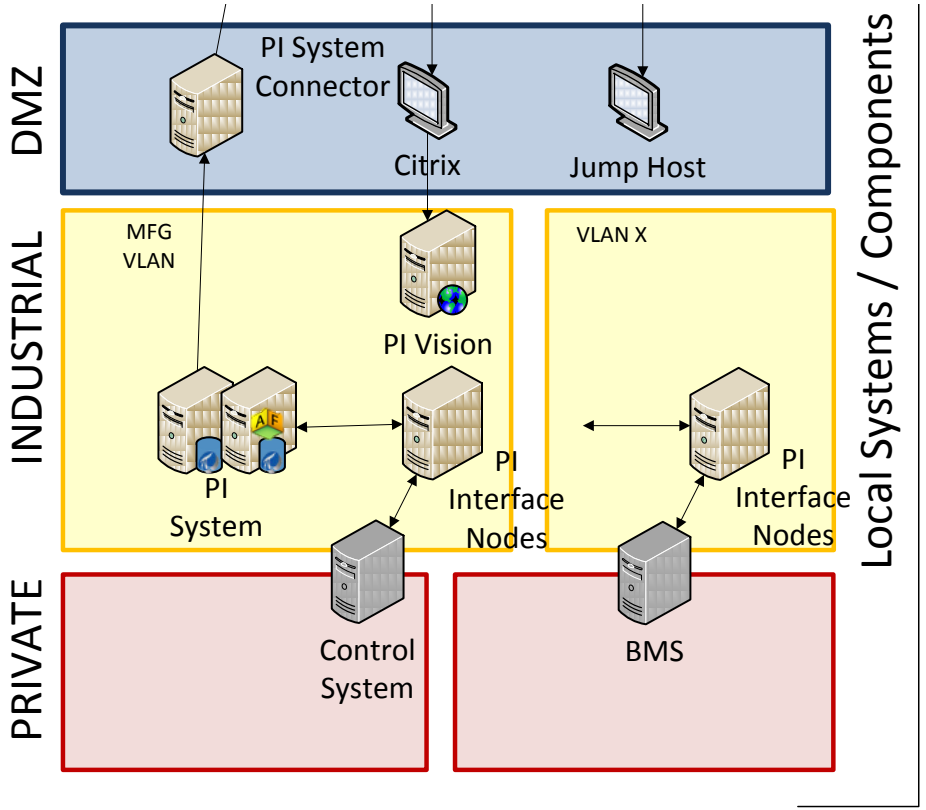
The PI System Connector resides within our DMZ to allow replicated data to be proxied out of the MCN to the Enterprise PI Server. The PI Connector Relay is in our Enterprise layer.



©2018 OSIsoft, LLC

Access at Site Level Gives us…

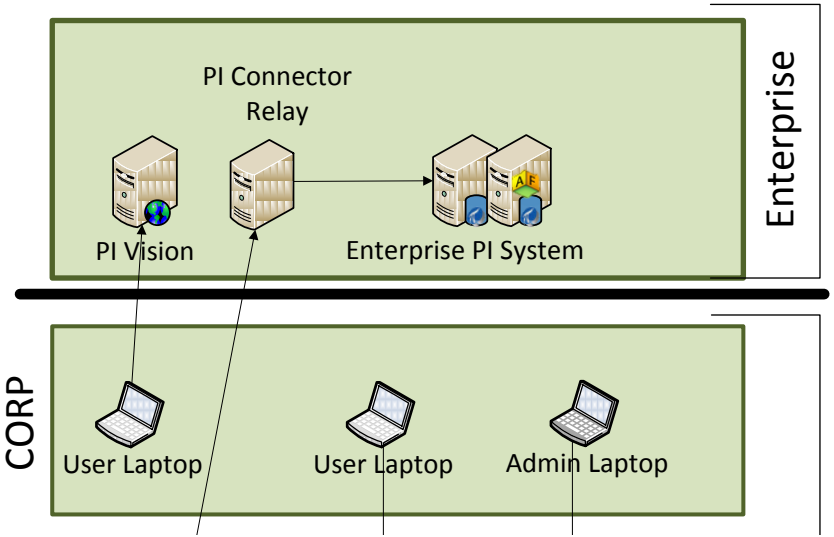
- Ensures access during WAN Outage
- Access through Citrix for Security
- Keeps MFG access within MCN



©2018 OSIsoft, LLC

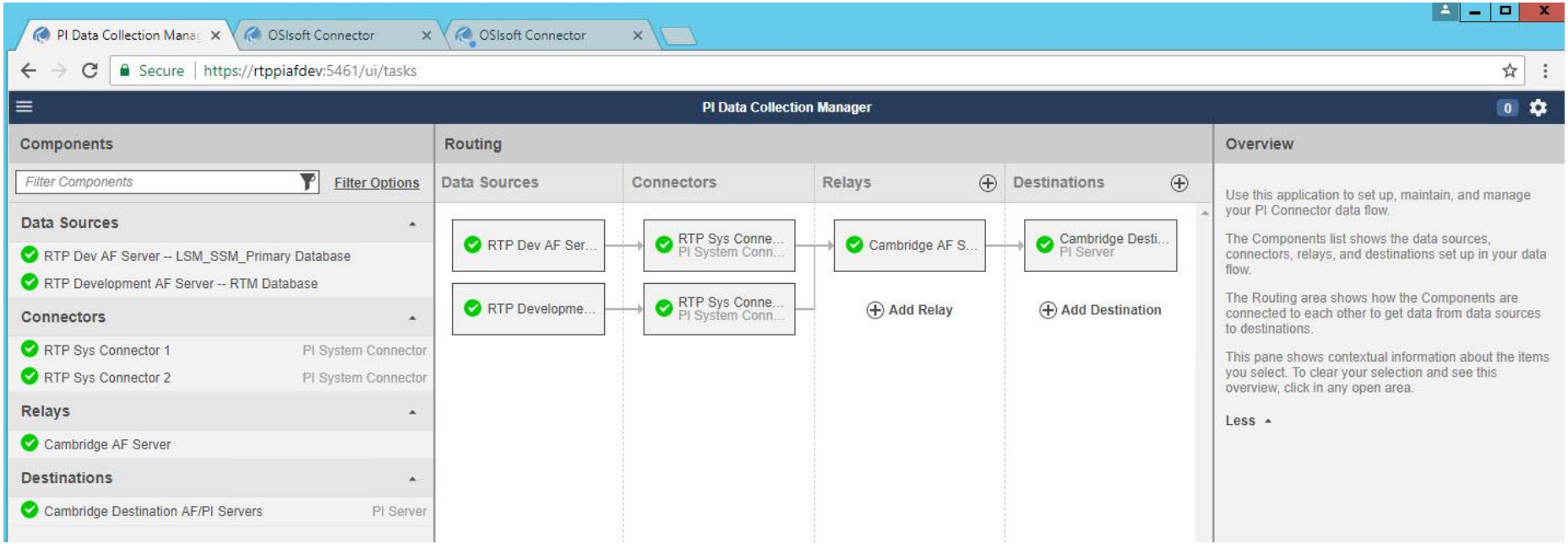
Access at Enterprise Level Gives us…

- User access above the firewall
- Utilize cloud computing
- Enterprise systems access replicate



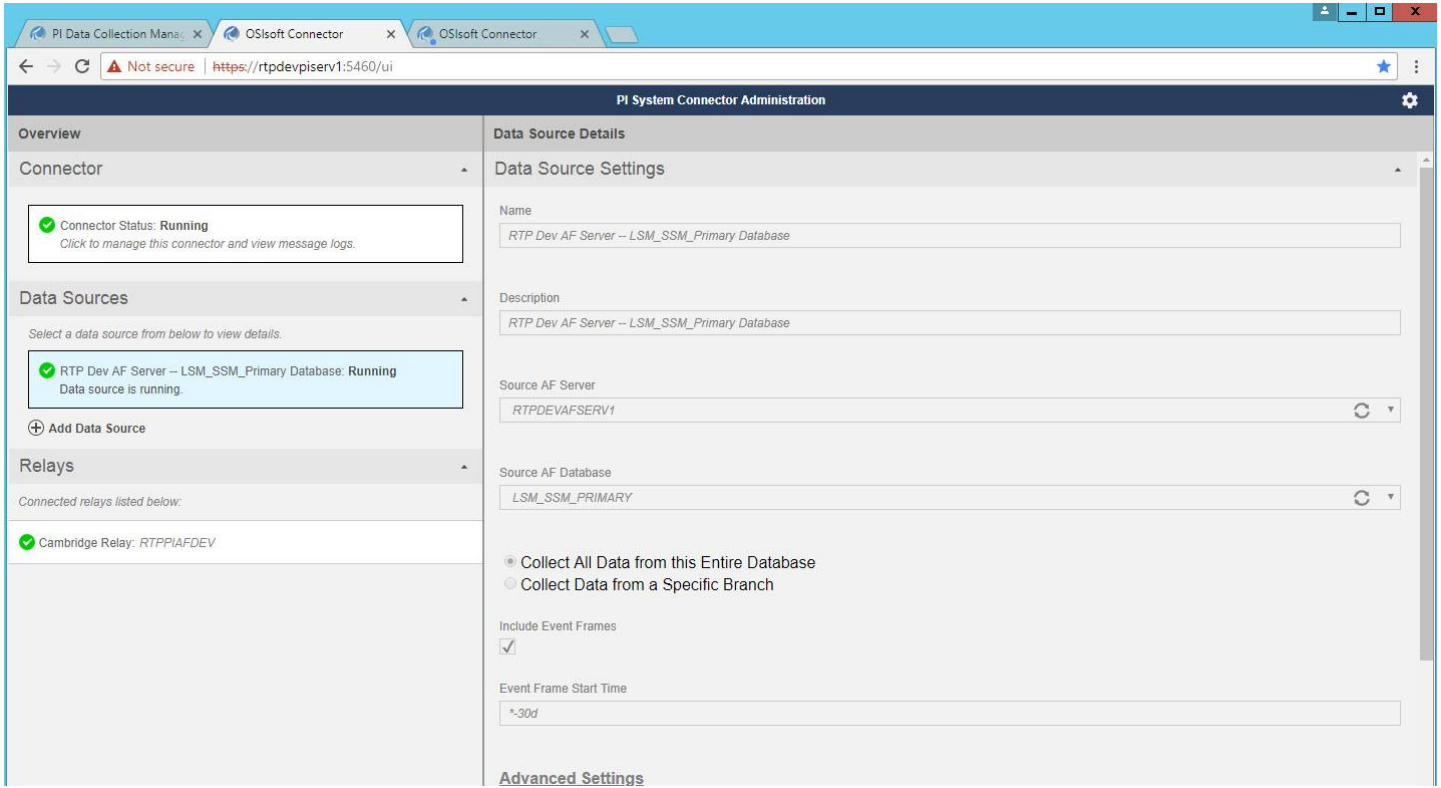
©2018 OSIsoft, LLC

PI System Connector Setup – Define Collections



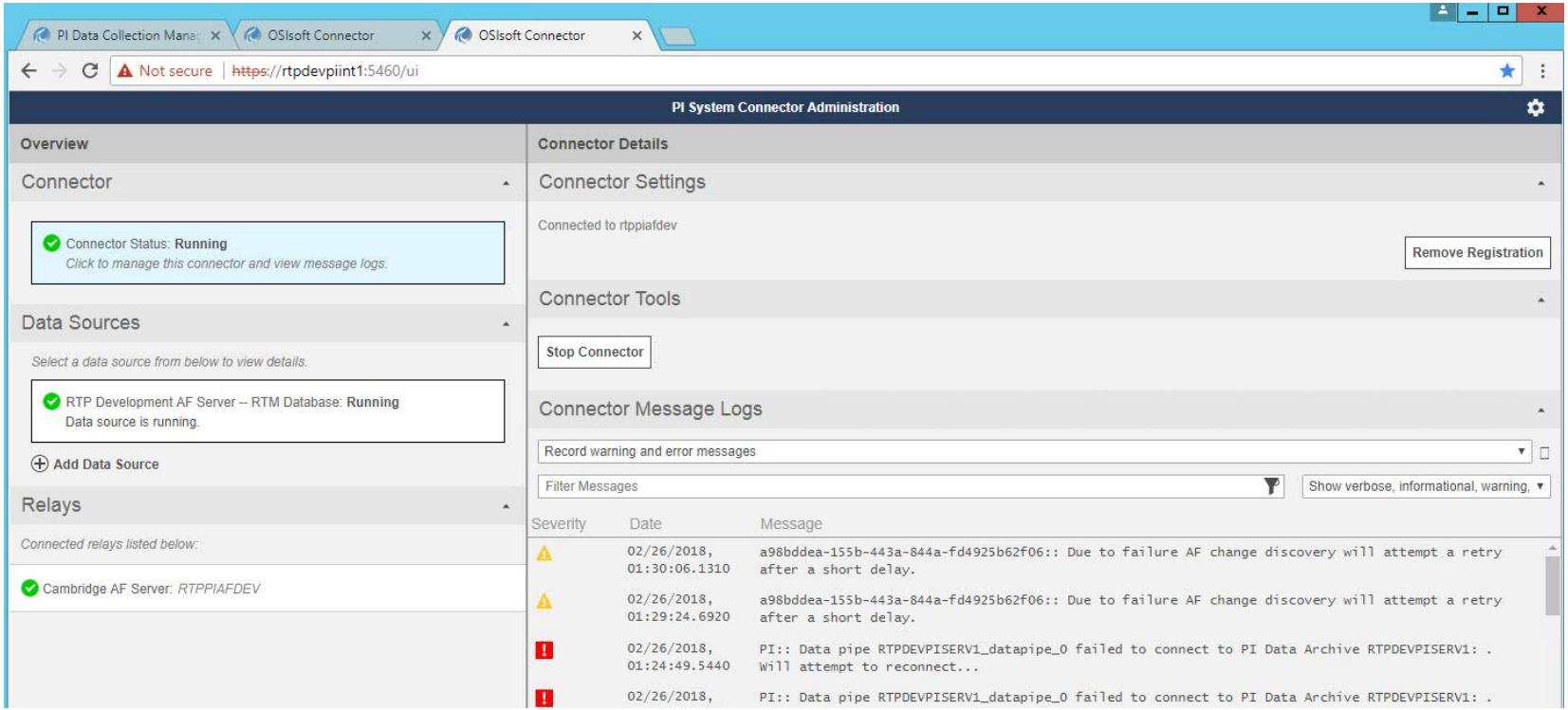
©2018 OSIsoft, LLC

PI System Connector Setup - Administration



©2018 OSIsoft, LLC

PI System Connector Setup – Message Logs



©2018 OSIsoft, LLC

Limitations on Initial Release

- Each AF Database requires its own PI System Connector on a separate VM.
- Snapshot data not replicated to destination server, only archived data/events.
- Event/archive edits and deletions on source are not picked up on destination.

©2018 OSIsoft, LLC

Enterprise Agreement Advantage

- Licensing for full replicate is expensive
- Utilize Site PI System for real-time calculations
- Utilize Enterprise PI System for access

Enterprise Agreement was the most cost effective solution!

©2018 OSIsoft, LLC

Role of Data Replication in Security



Create a Strong Security Posture for our Manufacturing Control Network (MCN)

CHALLENGE

Need to build a strong security posture for our MCN

- How to reduce the surface area of attack
- Provide data accessibility

SOLUTION

Evaluation was done on the entire network with new guidance and architecture provided

- Engineering and IT worked together to create best practices
- Third party evaluation of network
- Guidance created to enforce rules
- PI System Connector Development

RESULTS

MCN security posture strengthened through proper data flow

- Guidance provides consistency in network design
- Hardened network reduces security risks
- Replication of data to the Business Layer for access

©2018 OSIsoft, LLC

Contact Information



Gus Green

Gus.green@Biogen.com

https://www.linkedin.com/in/gustav-green-62700112/

Manager – Automation Systems Team
RTP, Biogen

- *Acknowledgements:* Frank Burrows, Leon Rice, Brandon Patton, Nate Bowman, Jason Dely, Tim Alosi

©2018 OSIsoft, LLC

Questions

Please wait for the **microphone** before asking your questions



State your **name & company**

Please remember to…

Complete the Online Survey for this session



©2018 OSIsoft, LLC

Merci

谢谢

Danke

Спасибо

Gracias

Thank You

감사합니다

ありがとう

Grazie

Obrigado

Optional: Click to add a takeaway you wish the audience to leave with.

©2018 OSIsoft, LLC